附件1

山东省教育行业网络与信息安全管理基本标准

一级指标	二级指标	指标标准	指标说明	权重
1．组织领导	1.1 管理机构	建立网络安全与信息安全工作领导机构； 明确本单位网络信息安全工作负责人。	以正式文件明确信息安全管理部门及信息安全主管领导、指定专职网络信息安全管理员。	5
	1.2 责任落实	明确网络与信息安全主体责任。	单位内部责任明确,安全到人、责任到岗。职能部门负责网络与信息安全工作的管理落实；技术支撑部门负责网络与信息安全防护体系建设、运行维护和技术支持等日常管理。	5
2．建设运维	2.1 制度建设	制定实施完备的网络与信息安全规范与制度。	建立信息安全管理制度体系，包括网络计算机软硬件管理、网站和信息系统建设与运维管理、数据安全及使用管理、人员安全管理等制度。	5
	2.2 等级保护	全面实施信息安全等级保护制度，提升信息系统安全管理的规范性和安全防护水平。	已有系统进行准确的定级和备案，按要求进行等保测评和问题整改。对新建信息系统，同步实施安全等级保护工作的定级、备案、测评和整改工作，确保安全防护措施到位。	8
	2.3 人员管理	强化各层面人员的安全管理。严格做好权限的授予、收回（调整），涉及重要数据的相关人员签订保密协议。	制定系统开发人员、网络管理员、系统管理员和使用人员等各层面人员的安全管理制度，及包括集成开发商和服务提供商等第三方人员的监督管理制度，做好权限划分、运维流程、操作回溯、密码管理和监督机制等各方面的规程完善和管理落实。	6
	2.4 应急管理	制定安全应急预案机制，定期开展安全应急演练。	制定安全事件的通知通报和安全应急预案机制，明确应急处置流程和权限，落实应急处置技术支撑队伍； 每年度开展二次应急演练，提供应急演练方案、演练记录、演练总结等相关文件并保存，提高网络与信息安全应急处置能力，发生事件能够按照应急处置程序进行迅速准确处置。	4
	2.5 建设整合	强化对信息化软硬件设施的建设应用整合。	对业务部门更多的提供 SaaS 服务，减少 PaaS 服务尤其是减少 IaaS 服务，加强网络和信息系统的集中管理和安全的统一运维。	2

一级指标	二级指标	指标标准	指标说明	权重
3．安全防护	3.1 物理安全	计算机机房必须符合GB/T2887-2011《计算机场地通用规范》C 级机房的相关要求，中心机房配备门禁系统或有专人值守，定期巡检。	中心机房必须专室专用，配备空调、UPS、防火防盗设施、温湿度设施、防静电地板、接地措施，配置电子门禁系统，控制、鉴别和记录人员出入，定期巡检机房设备，发现问题及时修复； 机房划分区域进行管理，区域之间设置物理隔离装置，在重要区域前设置等过渡区域。	7
	3.2 网络安全	设备和网络配置冗余，保障结构安全； 部署网络安全设备，配备访问控制策略； 部署网络设备状态监测系统和用户网络行为日志审计系统； 部署入侵检测防范和恶意代码防范系统，对网络设备进行防护。	保证网络设备的业务处理能力具备冗余空间，满足业务高峰期需要，接入网络和核心网络的带宽满足业务高峰期需要； 网络边界部署访问控制设备和入侵检测设备，阻断非授权访问并定期更新规则库； 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录，保存不少于 6 个月； 当检测到攻击行为时，应记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警及自动采取相应动作； 在网络边界处对恶意代码进行检测和清除，及时维护恶意代码库的升级和检测系统的更新； 对登录网络设备的用户采取身份鉴别等限制措施。	8
	3.3 主机安全	启用访问控制功能，配置唯一标识管理用户账号，并限制登录范围； 设备终端设置口令策略； 部署安全审计设备、日志分析服务器，部署防病毒设施，并定期更新； 对接入本单位网络的终端计算机进行认证。	为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性； 管理用户身份标识应具有不易被冒用的特点，配置强口令并定期更换； 设定终端接入方式、网络地址范围等条件限制终端登录； 根据信息系统的统一安全策略，实现集中审计，审计范围应覆盖到服务器上的每个操作系统用户和数据库用户； 部署防病毒网关或统一安装防病毒软件，并定期更新恶意代码库。收集关键设备日志并分析存在的安全风险； 采取技术措施对接入本单位网络的终端计算机进行认证。	7

一级指标	二级指标	指标标准	指标说明	权重
3．安全防护	3.4 应用安全	重要应用系统必须开展等级保护工作； 重要应用系统实现并配置严格的用户认证及授权策略，符合授权最小化原则； 对应用系统重要安全事件进行审计。	重要应用系统正式上线前进行安全检测并开展等级保护工作； 重要应用系统启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并应授予不同账户为完成各自承担任务所需的最小权限； 提供覆盖到每个应用系统用户的安全审计功能。	7
	3.5 数据安全	能够检测数据完整性； 做好网络设备、服务器、应用系统、数据库等重要设备和系统的数据备份工作； 采用加密或其他保护措施实现数据的存储保密性。	应能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施； 对重要设备的配置文件、操作系统、应用系统信息、数据库等进行本地和异地备份，在出现问题时能够快速恢复； 采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性。	7
4．网站安全	4.1 运维管理	落实网站备案管理制度。	开办网站应由单位主管领导审批，明确网站服务内容，按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，网站负责人、管理人员发生变动应及时重新备案或更新信息。	3
	4.2 安全防护	配置网站篡改防护设备，定期开展网站漏洞监测及日志分析。	单位及下属部门设立的门户网站应配置信息篡改的检测与防护措施；定期对网站进行安全漏洞扫描，及时进行修补；网站应开展日常或实时监测，日志分析；关闭存在严重安全风险的网站，阶段性使用的网站仅在使用期间开启。	4
	4.3 信息发布	网站信息发布前采取内容核查、审批等安全管理措施。	网站发布系统具备审核管理功能。	2
	4.4 记录日志	应用系统实现操作记录日志功能。	操作记录日志包括应用系统的关键操作事件。	2

一级指标	二级指标	指标标准	指标说明	权重
5．基础保障	5.1 队伍建设	加强网络安全管理队伍建设，建立岗前培训和岗位继续教育制度，提高全体人员的网络安全意识，提升从业人员的职业技能和水平。	建立网络与信息安全管理专职队伍和技术支撑专业队伍，落实岗位责任和考核机制；每年开展二次以上网络安全专题教育及业务培训活动。	4
	5.2 安全投入	加大安全投入，建立网络与信息安全经费投入机制。	设立网络与信息安全专项经费，额度大于年度信息化建设语段的10%，重点支持信息安全等级保护、安全防护能力建设、信息安全服务、人员培训等工作。	5
	5.3 安全检查	注重安全检查，定期开展网络与信息安全检查工作。	通过内部自查和远程安全检测等形式，做到尽早发现、提前防范、及时补救，建立考核与奖惩机制，确保工作落到实处。	5
	5.4 宣传教育	加强宣传教育，提高防范能力。	开展形式多样、针对性强的全员宣传教育，牢固树立网络与信息安全意识和政治意识、责任意识、保密意识，提高领导干部、管理人员、技术人员、教师的安全和防范意识；将网络安全教育工作作为安全教育的重要内容。	4